

UNITED STATES DISTRICT COURT

for the
Western District of Virginia

JAN 14 2011

JULIA C. DUDLEY, CLERK

BY:

DEPUTY CLERK

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

Hotmail email account

Case No.

7:10m414

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California (identify the person or describe the property to be searched and give its location):

The email account [REDACTED] maintained by MSN Hotmail of 1065 La Avienda, Mountain View, CA 94043.

The person or property to be searched, described above, is believed to conceal (identify the person or describe the property to be seized):

See Attachment B (copy attached) of the Affidavit, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☒ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation(s) of 18 U.S.C. §, 1201 (a), and the application is based on these facts:

☒ Continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SA T. David Church

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/10/10

City and state:

Roanoke, VA

Judge's signature

Michael F. Urbanski

United States Magistrate Judge

Printed name and title

JAN 14 2011

IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF VIRGINIA

JULIA C. DUDLEY, CLERK
BY: *[Signature]*
DEPUTY CLERK

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
[REDACTED] THAT ARE
STORED AT PREMISES CONTROLLED BY
HOTMAIL

Case No. 7:10m 414

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Special Agent T. David Church, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Hotmail an e-mail provider headquartered at Hotmail, 1065 La Avenida, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Yahoo! to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent of the Federal Bureau of Investigation (FBI). I have been employed as a Special Agent since October 15, 1996, and I am currently assigned to the FBI's Richmond Field Division, Roanoke Resident Agency, Roanoke, Virginia. As a Special Agent of

the FBI, I have performed a variety of investigative tasks, including functioning as a case agent in cases involving Violent Crimes, Civil Rights violations, Fraud against the Government, Terrorism investigations, Computer related crimes, and numerous other violations. Based upon my training and experience as a Special Agent of the FBI, I know that the Internet is a global network of computers and other electronic devices that communicate with each other via standard telephone lines, high-speed telecommunications links (e.g., fiber optic cable), and wireless transmissions. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

3. Every device on the Internet has an address that allows other devices to locate and communicate with it. An Internet Protocol (IP) address is a unique number that identifies a device on the Internet. Other addresses include Uniform Resource Locator (URL) addresses, such as "http://www.usdoj.gov," which are typically used to access web sites or other services on remote devices. Domain names, host names, and machine addresses are other types of addresses associated with Internet use. Many individuals and businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP.

4. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with it. Those records could include identifying and billing information,

account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data format and in written record format. ISPs reserve and/or maintain computer disk storage space on their computer system for the use of the Internet service subscriber for both temporary and long-term storage of electronic communications with other parties and other types of electronic data and files. E-mail that has not been opened is stored temporarily by an ISP incident to the transmission of the e-mail to the intended recipient, usually within an area known as the home directory. Such temporary, incidental storage is defined by statute as “electronic storage,” and the provider of such a service is an “electronic communications service” provider. A service provider that is available to the public and provides storage facilities after an electronic communication has been transmitted and opened by the recipient, or provides other long term storage services to the public for electronic data and files, is providing a “remote computing service.”

5. Most services offered on the Internet assign users a name or ID, which is a pseudonym that computer systems use to keep track of users. User names and IDs are typically associated with additional user information or resources, such as a user account protected by a password, personal or financial information about the user, a directory of files, or an email address.

6. In my training and experience, I have learned that Hotmail provides a variety of on-line services, including electronic mail (“e-mail”) access, to the general public. Subscribers obtain an account by registering with Hotmail. During the registration process, Hotmail asks subscribers to provide basic personal information. Therefore, the computers of Hotmail are

likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Hotmail subscribers) and information concerning subscribers and their use of Hotmail services, such as account access information, e-mail transaction information, and account application information.

7. In general, an e-mail that is sent to a Hotmail subscriber is stored in the subscriber's "mail box" on Hotmail servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Hotmail servers indefinitely.

8. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Hotmail's servers, and then transmitted to its end destination. Hotmail often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Hotmail server, the e-mail can remain on the system indefinitely.

9. A Hotmail subscriber can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by

10. Subscribers to Hotmail might not store on their home computers copies of the e-mails stored in their Hotmail account. This is particularly true when they access their Hotmail account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

11. In general, e-mail providers like Hotmail ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and

other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

12. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

13. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

14. In my training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.

PROBABLE CAUSE

15. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

16. [REDACTED] lived at [REDACTED] [REDACTED] via. [REDACTED]'s boyfriend, Jeffrey Scott Easley, also lived with [REDACTED] since July 2010. On Friday, December 3, 2010 and Monday December 6, 2010, [REDACTED] was absent from school.

17. On December 6, 2010, at approximately 9:30 a.m., [REDACTED] with was found lying dead in her home by a co-worker who was concerned that [REDACTED] had not shown up to work on either Sunday or Monday. [REDACTED] had presumably been murdered, as her body was bound, and there were indications of blunt force trauma to her head. Both [REDACTED] and Easley were missing and law enforcement believes [REDACTED] may have been abducted by Easley. Their whereabouts are currently unknown.

18. On December 7, 2010, the General District Court for Roanoke County issued an arrest warrant for Jeffrey Scott Easley for a violation of Section 18.2-47, Code of Virginia, (Kidnapping).

19. On December 6, 2010, the Roanoke County Police Department requested assistance from the Federal Bureau of Investigation, Roanoke Division, in locating and apprehending Jeffrey Scott Easley and safely recovering [REDACTED]

20. The investigation so far has revealed the following: [REDACTED] was last seen alive about 8:45 a.m. on Friday, December 3, 2010, at a doctor's appointment. Her daughter [REDACTED] was with her at this appointment. The last communication of any kind with [REDACTED] was on Friday, December 3, 2010, when she rescheduled another medical appointment. On Friday evening, December 3, 2010, bank surveillance equipment showed Easley withdrawing \$400 from [REDACTED] bank account at the SunTrust Bank automated teller machine (ATM) in Salem, Virginia. That same evening, Easley attempted to withdraw money from [REDACTED] bank account at a Member One Federal Credit Union ATM in Salem, Virginia. Bank surveillance equipment showed an individual believed to be [REDACTED], in Easley's vehicle at the time, described as a red 2000 Chevrolet Blazer, Virginia tag [REDACTED]. That same evening, Easley and [REDACTED] were seen in a Wal-Mart store in Salem, Virginia, purchasing camping supplies with [REDACTED] credit card.

21. On December 3, 2010, Easley sold his 2000 Chevrolet Blazer, Virginia tag [REDACTED] to a couple from Roanoke, Virginia. Following the sale, the purchasers observed an unidentified male pick up Easley and an individual believed to be [REDACTED] vehicle, described as a silver [REDACTED] Dodge Neon, Virginia tag [REDACTED] is currently missing.

22. Investigators have determined that at the time [REDACTED] was killed [REDACTED] Jeffrey Easley and [REDACTED] had active MySpace accounts: [REDACTED] User ID [REDACTED] Jeffrey Easley User ID [REDACTED] and [REDACTED] User ID [REDACTED]. On December 6, 2010, records received from MySpace pursuant to an authorized Emergency Disclosure request, revealed the following message string from User ID [REDACTED] (Jeffrey Easley) to User [REDACTED] ([REDACTED]) which took place the morning that [REDACTED] was last seen alive.

Date	Time	Message
12/02/2010	9:07pm EST	"yes or no?"
12/03/2010	7:22am EST	"ur mom wants me 2 leave this morning"
12/03/2010	8:31am EST	"when u get back im going 2 do it I cant lose u sweetheart"

23. Additionally, the records received from MySpace revealed that User ID [REDACTED] is subscribed to by Jeff Easley and has an associated e-mail of [REDACTED] and User [REDACTED] is subscribed to by [REDACTED] and has an associated e-mail of [REDACTED]

24. A review of social networking websites associated with [REDACTED] has revealed that [REDACTED] has informally changed her last name to Easley on some of her social network accounts.

25. Investigators have determined that at the time [REDACTED] was killed, [REDACTED] Jeffrey Easley and [REDACTED] also had active Facebook accounts: [REDACTED] # [REDACTED] Jeffrey Easley's User ID [REDACTED] and [REDACTED]'s URL [REDACTED] On December 6, 2010, records received from Facebook pursuant to an authorized Emergency Disclosure request, identified that [REDACTED] (Jeffrey Easley) is associated with [REDACTED] and User ID [REDACTED] [REDACTED] is associated with [REDACTED]

26. On December 7, 2010, records received from America On Line (AOL) document that [REDACTED] is subscribed to by Jeff Easley, [REDACTED], Virginia. A search conducted of a subscription database identified this address as the residence of Jeff Easley's step-father and mother.

27. A review of e-mail and social networking websites belonging to Jeffery Easley and [REDACTED] has made it apparent that both frequent social networking websites, such as Facebook, MySpace, MSN Hotmail, Yahoo, and AOL, on a daily basis.

28. A forensic search of [REDACTED] laptop computer discovered the Yahoo user name of [REDACTED]. The e-mail address [REDACTED] is attributed to [REDACTED]. [REDACTED] in several received e-mails associated with her daughter [REDACTED] e-mail account [REDACTED].

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

29. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Hotmail to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

30. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of Hotmail there exists evidence of a crime and contraband or fruits of a crime. Accordingly, a search warrant is requested.

31. This Court has jurisdiction to issue the requested warrant because it is "a court with jurisdiction over the offense under investigation." 18 U.S.C. § 2703(a).

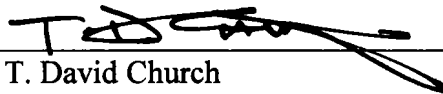
A14

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING

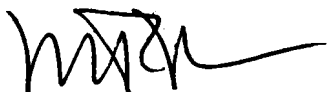
33. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



T. David Church
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on December 10, 2010:




MICHAEL F. URBANSKI
UNITED STATES MAGISTRATE JUDGE

A14

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with e-mail account

 that is stored at premises owned, maintained, controlled, or operated by Hotmail, an e-mail provider headquartered at Hotmail, 1065 La Avenida, Mountain View, California 94043.

414

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Hotmail

To the extent that the information described in Attachment A is within the possession, custody, or control of Hotmail, Hotmail is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
- d. All records pertaining to communications between Hotmail and any person regarding the account, including contacts with support services and records of actions taken.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violation of Title 18, United States Code, Section 1201(a) involving Jeffrey Scott Easley since January 1, 2010, including, for each user ID identified on Attachment A, information pertaining to the following matters:

- (a) Preparatory steps taken in furtherance of the crime, including any postings by and communications between Jeffrey Scott Easley and [REDACTED]
- (b) Records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts.

A14

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC
BUSINESS RECORDS PURSUANT TO FEDERAL RULE
OF EVIDENCE 902(11)**

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by America On Line and my official title is _____. I am a custodian of records for America On Line. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of America On Line, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

- a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;
- b. such records were kept in the ordinary course of a regularly conducted business activity of America On Line; and
- c. such records were made by America On Line as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

Date

Signature